[ポスター発表] 研究報告

# トリアージを取り入れたサーバに関するセキュリティインシデントの対応支援システムの検討

森 公希[1]　新城 靖[2]　中井 央[3,4]　三宮 秀次[2,4]　佐藤 聡[2,4]

# A Study on a Support System for Server Incident Response Based on Triage

## 1. はじめに

近年，DoS 攻撃，乗っ取り，機密情報の搾取などの不正アクセス増加に伴い，大学や企業などの組織では IDS(侵入検知装置) や脆弱性検査装置が普及している．

IDS は不正アクセスの検知が可能であり，検知した内容はセキュリティアラートとしてネットワーク管理者に通知されるが，必ずしも検知した攻撃が成功しているとは限らない．脆弱性検査装置はネットワーク内のサーバが保有する既知の脆弱性を把握可能である．IDS が検知した攻撃は，サーバの保有しない脆弱性が対象であれば成功していない．また，保有している脆弱性を対象とした攻撃の場合でも，サーバ管理者が何らかの対策を行っている場合には成功していない．しかし，大学等のようにネットワーク内のサーバを管理するサーバ管理者とネットワーク全体を管理するネットワーク管理者が異なる大きな組織においては，ネットワーク管理者はサーバ管理者が対策を行っているかまでは把握が難しく，ネットワーク管理者によるサーバ管理者への問い合わせが必要となる．そこで，本研究では，ネットワーク管理者が対応すべきアラート数を減らすことを目的とし，脆弱性検査結果とサーバ管理者に問い合わせた結果を記録・活用し，セキュリティアラート毎にサーバのトリアージを行うセキュリティインシデントの対応支援システムを提案する．

1 筑波大学大学院博士前期課程システム情報工学研究科コンピュータサイエンス専攻
Master ’ s Program in Computer Science, Graduate School of Systems and Information Engineering, University of Tsukuba.
2 筑波大学システム情報系
Faculty of Engineering, Information and Systems, University of Tsukuba.
3 筑波大学図書館情報メディア系
Faculty of Library, Information and Media Science, University of Tsukuba.
4 筑波大学学術情報メディアセンター
Academic Computing and CommunicationsCenter, University of Tsukuba.

## 2. 提案手法

インシデント対応におけるトリアージとは，組織の活動ポリシーによって定められた基準を元に，インシデント対象の優先度を決定することで迅速な対応を行うための手法である [1]．本研究におけるトリアージは，IDS のアラートと脆弱性検査結果の情報に加えて，ネットワーク内にある各サーバの保有する各種脆弱性への対応状態を用いることで，インシデント対象のサーバに対応する優先度を決定することとする．

**図 1** に本研究で提案するシステムの構成を示す．まず，IDS のアラート情報から脆弱性識別子を特定する．IDS のアラート情報から取得できる項目として，

- 検知時刻
- 送受信先の IP アドレス
- クライアント・サーバ間の通信方向
- アラートの重大度
- 脆弱性識別子（例. CVE など）

を想定する．これら項目は間接的に取得できるものを含んでよいものとする．

次に脆弱性検査結果により，アラートが検知した攻撃が対象とする脆弱性をサーバが保有しているかを確認し，保有していればサーバ管理者に対してヒアリングを行い，脆弱性への対応状態を更新する．ヒアリングの内容は，

- 脆弱性に関する対策を行っているか
- サーバ内で重要データを取り扱っているか

の 2 つとする．重要データを取り扱っているか否かのヒアリングは，アラート受信時にすぐ対応すべきサーバであるかを判断するため必要となる．

脆弱性への対応状態の管理により，同様の脆弱性に関してのアラートの分類が可能となる．また，ネットワーク管理者は組織の活動ポリシーに応じて，サーバの重要度を変更する条件をルールとして追加できる．

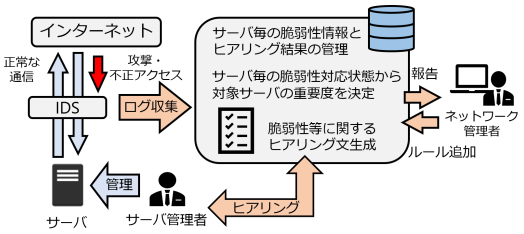


**図 1** 提案システムの構成
**Fig. 1** A structure of the proposed system

| | 脆弱性の保有 | ヒアリング済み | ヒアリング結果 |
|---|---|---|---|
| 無視可能なアラート | × | − | − |
| | ○ | ○ | ○ |
| 調査すべきアラート | ○ | × | − |
| 制限すべきアラート | ○ | ○ | × |
| | 脆弱性検査に未対応 | − | − |

（○：該当あり，×：該当なし，−：決定に関係なし）

**図 2** アラートの分類条件
**Fig. 2** Alert classification condition

## 3. アラートの分類

**図 2** に，脆弱性への対応状態に基づいたアラートの分類条件を示す．「無視可能なアラート」は，サーバが脆弱性検査結果として脆弱性を保有していない，または脆弱性を保有しているがすでにサーバ管理者によって対策済みである場合に分類する．「調査すべきアラート」は，脆弱性を保有しているがサーバ管理者へのヒアリングが未実施である，またはヒアリングに未回答の場合に分類する．また，最初に通知される脆弱性は必ず「調査すべきアラート」に分類する．「制限すべきアラート」は，脆弱性を保有しており，未対策である場合に分類する．また，脆弱性を保有しない場合でも IDS による検知結果として重大なアラートであると判断された場合は脆弱性検査に未対応の脆弱性であると判断し，「制限すべきアラート」に分類する．

## 4. 対応状態に基づくトリアージ

**図 3** に脆弱性毎でのサーバの対応状態の遷移を示す．最初に検知する脆弱性は「調査すべきアラート」のため，初期状態は「調査中」であり，サーバ管理者へのヒアリングが行われ，その結果，対策済みであれば「無視可能」に，未対策であった場合は，重要データの有無で「調査中」か「制限中」に遷移させる．「制限すべきアラート」を受信した場合は，どの状態であっても「制限中」に遷移させる．「制限中」になると，ネットワーク管理者へ通知される．「制限中」は，ネットワーク管理者による対応により「無視可能」へと遷移させることができる．

ネットワーク管理者は，アラートの分類に別途ルールを追加することができる．ルール追加の例として，**図 4** に

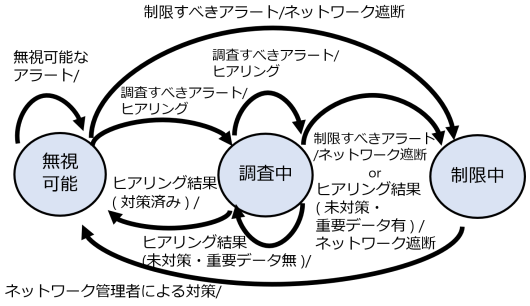


**図 3** 脆弱性の対応状態の遷移
**Fig. 3** Vulnerability response state transition

| | 脆弱性の保有 | ヒアリング結果 | 一定回数受信 |
|---|---|---|---|
| 無視可能なアラート | × | − | − |
| | ○ | ○ | − |
| 調査すべきアラート | ○ | − | − |
| 制限すべきアラート | ○ | × | − |
| | 脆弱性検査に未対応 | − | − |
| | ○ | × | ○ |

**図 4** アラート分類に関するルール追加
**Fig. 4** Rule addition for alert classification

「脆弱性を保有しており，その脆弱性のアラートを一定回数受信した場合に制限すべきアラートに分類する」というルールを追加した分類条件を示す．このルールの追加によって，サーバ管理者へのヒアリングの回答が返ってこない場合や，同様の脆弱性に関するアラートが高頻度で受信された場合に対象サーバの優先度を意図的に高くすることで対応できる．

## 5. おわりに

今後は，過去のログを用いて提案手法をシミュレーションする．ログは大学で運用した Palo alto Networks 社製のファイアウォールログ [2] を 1 か月分使用し，Nessus Professional による脆弱性検査結果 [3] を合わせて利用する．部分的な評価として，ネットワーク管理者に通知されるアラート数とサーバ管理者へのヒアリング数がどれだけ減ったかを比較する．

### 参考文献

[1] 一般社団法人 JPCERT コーディネーションセンター, インシデントハンドリングマニュアル, [online] https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf (参照 2019-10-2).
[2] Palo Alto Networks, Threat Log Fields [online] https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/threat-log-fields.html# (参照 2019-10-2).
[3] Tenable Network Security, Nessus Professional [online] https://jp.tenable.com/products/nessus/nessus-professional (参照 2019-10-2).